



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/463,907	02/02/2000	SHIHO MORIAI	0162/00547	6943

7590 11/03/2005
POLLOCK VANDE SANDE & AMERNICK
PO BOX 19088
WASHINGTON, DC 20036-3425

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT PAPER NUMBER

2131

DATE MAILED: 11/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/463,907

Applicant(s)

MORIAI ET AL.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 August 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 6,8,13-16,18-23,25,26,31 and 32 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 6,8,13-16,18-23,25,26,31 and 32 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 05 August 2005 has been noted and made of record.
2. Claims 6, 8, 13-16, 18-23, 25, 26, 31, and 32 have been presented for examination.
3. Claims 1-5, 7, 9-12, 17, 24, 27-30, and 33-38 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments filed 05 August 2005 have been fully considered but they are not persuasive.
5. In response to the Applicant's argument that Kim does not disclose the candidate function generating means generating candidate functions, each formed by a composite function composed of two different algebraic structures, the Examiner disagrees. Kim broadly discusses generating a substitution box that is secure against differential and linear cryptanalysis, see column 1, lines 35-42. The Examiner contends that it is well known to use mathematical functions in choosing good, secure S-boxes. This is supported by **Applied Cryptography** by Bruce Schneier, hereinafter Schneier, on pages 349-351. Schneier states that math-made S-boxes are chosen according to mathematical principles so that they have proven security against differential and linear cryptanalysis and good diffusive properties. This is further supported by **Differentially uniform mappings for cryptography**, which provides proof of algebraic functions providing for secure s-boxes that are secure against differential and linear cryptanalysis with good diffusive properties.
6. Therefore, Kim discloses generating S-boxes using mathematical functions.
7. See further rejections that follow.

Claim Rejections

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claim 6 is rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,796,837 to Kim et al., hereinafter Kim.

10. As per claim 6, Kim teaches a random function generating apparatus for a data encryption device comprising:

input means for inputting digital signals representing parameter values of each of a plurality of functions each of a composite function composed of first and second functions of different algebraic structures, and for storing them in storage means (Figures 6 [blocks 602, 603, 604], 7 [blocks 702, 703], 8 [blocks 802, 803], 9 [blocks 902, 903], 10a [blocks 1002, 1003, 1004, 1005, 1006], 10b [blocks 1019, 1020, 1021, 1022], 11 [block 1102, 1103], 12 [block 1202, 1203]; column 1, lines 35-42; column 4, lines 1-9; column 4, lines 12-28; column 4, lines 41-63);

candidate function generating means for generating candidate functions each of said composite function formed of said first and second functions of different algebraic structures based on said plurality of parameters read out of storage means (Figures 6 [blocks 602, 603, 604], 7 [blocks 702, 703], 8 [blocks 802, 803], 9 [blocks 902, 903], 10a [blocks 1002, 1003, 1004, 1005, 1006], 10b [blocks 1019, 1020, 1021, 1022], 11 [block 1102, 1103], 12 [block 1202, 1203]; column 1, lines 35-42; column 4, lines 1-9; column 4, lines 12-28; column 4, lines 41-63);

resistance evaluating means for evaluating the resistance of each of said candidate functions to a cryptanalysis (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023,

Art Unit: 2131

1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks 1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4, lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13); and

selecting means for selecting those of said resistance-evaluated candidate functions which are highly resistant to said cryptanalysis and outputting digital signals representing selected ones of said resistance-evaluated candidate functions (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks 1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4, lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13);

wherein one of said first and second functions of different algebraic structures is resistant to each of differential cryptanalysis and linear cryptanalysis (column 4, lines 12-62).

11. Claims 8, 13, 14-16, 18-23, 25, 26, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim in view of **The Interpolation Attack on Block Ciphers**, by Thomas Jakobsen et al., hereinafter Jakobsen, as applied to claim 6 above, and further in view of **Partitioning Cryptanalysis**, by Carlo Harpes, hereinafter Harpes, in view of Langford.

12. Regarding claim 8, Kim discloses evaluating the resistance of said function to cryptanalysis based on the result of said number (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks

Art Unit: 2131

1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4, lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13);

13. Wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks 1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4, lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13).

14. Kim does not disclose using higher-order-differential cryptanalysis, interpolation-cryptanalysis, partitioning-cryptanalysis, and differential-linear cryptanalysis.

15. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use higher-order-differential cryptanalysis, since Jakobsen states in the Abstract that such a modification would be useful in detecting vulnerabilities of ciphers in low non-linear order. Therefore Jakobsen discloses calculating a minimum value of the degree of a Boolean polynomial for input bits by which output bits of each of said candidate functions are expressed, as discussed in **Section 2: Attacks Using Higher Order Differentials**.

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use interpolation-cryptanalysis, since Jakobsen states in the Abstract that such a modification would be useful in detecting vulnerabilities in ciphers that use simple algebraic functions. Therefore Jakobsen discloses expressing an output value y as $y = f_k(x)$ for an input

Art Unit: 2131

value x and a fixed key k using a polynomial over a Galois field which is composed of elements equal to a prime p or a power of said prime p and counting a number of terms of said polynomial in at least **Section 3: The Interpolation Attack**.

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use partitioning cryptanalysis, since Harpes states in the Abstract that such a modification would exploit a potential weakness of the cipher, namely that the last-round inputs are non-uniformly distributed over the blocks of the second partition when the plaintexts are taken from a particular block of the first partition. Therefore Harpes discloses dividing all input values of the function to be evaluated and the corresponding output values into input subsets and output subsets and calculating an imbalance of the relationships between the input subset and the output subset with respect to their average corresponding relationship on at least pages 7 and 8, in addition to **Sections 3-5**, on page 9-23.

18. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use differential-linear cryptanalysis, since Langford states on pages 17 and 18 that such a modification reduces the amount of text required in the analytic attacks. Therefore, Langford discloses counting all sets of input difference value Δx and output mask value Δy of each of the functions $S(x)$ read out of the storage means, a number of inputs values x for which the inner product of $(S(x)+S(x + \Delta x))$ and said output mask value Δy is 1, as illustrated by Figure 2, on page 21 and is discussed in **Section 5, Structures** on pages 23 and 24 .

19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include four cryptanalysis routines in one device, since it has been held that forming in one piece routines or techniques that were formerly found separately involves only routine

Art Unit: 2131

skill in the art. See MPEP § 2144.04; see *Howard v. Detroit Stove Works*, 150 U.S. 164 (1993); see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1965); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

20. As per claims 13 and 20, Kim teaches a random function generating method comprising the steps of:

(o) inputting digital signals representing input difference values $\square x$, output mask values $\square y$ and parameter values of each of a plurality of candidate functions and storing them in storage means (Figures 6 [blocks 602, 603, 604], 7 [blocks 702, 703], 8 [blocks 802, 803], 9 [blocks 902, 903], 10a [blocks 1002, 1003, 1004, 1005, 1006], 10b [blocks 1019, 1020, 1021, 1022], 11 [block 1102, 1103], 12 [block 1202, 1203]; column 1, lines 35-42; column 4, lines 1-9; column 4, lines 12-28; column 4, lines 41-63);

(a) setting various input values read out of the storage means for each of candidate functions $S(x)$ of S-box and calculating output values corresponding to said various input values x (Figures 6 [blocks 602, 603, 604], 7 [blocks 702, 703], 8 [blocks 802, 803], 9 [blocks 902, 903], 10a [blocks 1002, 1003, 1004, 1005, 1006], 10b [blocks 1019, 1020, 1021, 1022], 11 [block 1102, 1103], 12 [block 1202, 1203]; column 1, lines 35-42; column 4, lines 1-9; column 4, lines 12-28; column 4, lines 41-63);

(b) storing the output values in storage means (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks 1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4,

Art Unit: 2131

lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13); and

(c) evaluating the resistance of each of said candidate functions to a cryptanalysis based on values stored in said storage means, and selectively outputting candidate function highly resistant to said cryptanalysis (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks 1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4, lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13); and

21. Kim does not disclose using higher-order-differential cryptanalysis, interpolation-cryptanalysis, partitioning-cryptanalysis, and differential-linear cryptanalysis.

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use higher-order-differential cryptanalysis, since Jakobsen states in the Abstract that such a modification would be useful in detecting vulnerabilities of ciphers in low non-linear order. Therefore Jakobsen discloses calculating a minimum value of the degree of a Boolean polynomial for input bits by which output bits of each of said candidate functions are expressed, as discussed in **Section 2: Attacks Using Higher Order Differentials**.

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use interpolation-cryptanalysis, since Jakobsen states in the Abstract that such a modification would be useful in detecting vulnerabilities in ciphers that use simple algebraic functions. Therefore Jakobsen discloses expressing an output value y as $y = fk(x)$ for an input value x and a fixed key k using a polynomial over a Galois field which is composed of elements

Art Unit: 2131

equal to a prime p or a power of said prime p and counting a number of terms of said polynomial in at least **Section 3: The Interpolation Attack**.

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use partitioning cryptanalysis, since Harpes states in the Abstract that such a modification would exploit a potential weakness of the cipher, namely that the last-round inputs are non-uniformly distributed over the blocks of the second partition when the plaintexts are taken from a particular block of the first partition. Therefore Harpes discloses dividing all input values of the function to be evaluated and the corresponding output values into input subsets and output subsets and calculating an imbalance of the relationships between the input subset and the output subset with respect to their average corresponding relationship on at least pages 7 and 8, in addition to **Sections 3-5**, on page 9-23.

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use differential-linear cryptanalysis, since Langford states on pages 17 and 18 that such a modification reduces the amount of text required in the analytic attacks. Therefore, Langford discloses counting all sets of input difference value Δx and output mask value Δy of each of the functions $S(x)$ read out of the storage means, a number of inputs values x for which the inner product of $(S(x)+S(x + \Delta x))$ and said output mask value Δy is 1, as illustrated by Figure 2, on page 21 and is discussed in **Section 5, Structures** on pages 23 and 24 .

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include four cryptanalysis routines in one device, since it has been held that forming in one piece routines or techniques that were formerly found separately involves only routine skill in the art. See MPEP § 2144.04; see *Howard v. Detroit Stove Works*, 150 U.S. 164 (1993);

Art Unit: 2131

see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1965); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

27. Regarding claims 14 and 21, Kim discloses the use of differential and linear cryptanalysis, which includes predicting the probability of a successful attack. This is discussed in depth in **Block Cipher – Analysis, Design and Application**, by Lars Knudsen, hereinafter referred to as Knudsen, in at least **Sections 5.2 [Differential Cryptanalysis]** and **5.3 [Linear Cryptanalysis]**, as well as **Section 6.1.6 [Linear Cryptanalysis]**, specifically equation 6.2. Kim discloses a similar equation to that of equation 6.2 in column 4, lines 25-30. Thus the equation $\xi_s(\Box x, \Box y) = |2x\#\{x \in GF(2)^n | (S(x) + S(x + \Box x)) \cdot \Box y = 1\} - 2^n|$, is a part of differential-linear analysis as it appears to be a differentiated version of equation 6.2 of Knudsen. Therefore the s-box is evaluated with respect to Ξ , where Ξ is the probability of a successful attack being executed during the cryptanalysis routine.

28. Harpes discusses the principles behind a partitioning cryptanalysis attack on pages 7 and 8 and the probability of success of partitioning cryptanalysis, including imbalance, on pages 11-23. Therefore Harpes discloses the step of dividing an input value set F and an output value set G of said function into u input subsets $\{F_0, F_1, \dots, F_{u-1}\}$ and v output subsets $\{G_0, G_1, \dots, G_{v-1}\}$, for each partition pair (F_i, G_j) ($i = 0, \dots, u-1; j = 0, \dots, v-1$), calculating a maximum one of probabilities that all output values y corresponding to all input values x of the input subset F_i belong to the respective output subsets G_j ($j = 0, \dots, v-1$), and calculating a measure $IS(F, G)$ of an average imbalance of a partition-pair (F,G) based on all maximum values calculated for all partition pairs.

Art Unit: 2131

29. Kim discloses evaluating the resistance of said candidate function to said cryptanalysis based on said measure (Figures 6 [blocks 606, 607], 7 [block 704], 8 [block 804], 9 [blocks 904, 905], 10a [blocks 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014], 10b [blocks 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030], 11 [block 1105], 12 [blocks 1205], 13a [blocks 1305, 1306, 1307, 1308], 13b [blocks 1309, 1310, 1311]; column 4, lines 12-18; column 4, lines 31-62; column 5, lines 1-40; column 5, line 41 to column 6, line 13).

30. Regarding claims 15, 18, 22, and 25, Kim discloses setting aside candidate functions that fail the testing conditions. It would have been obvious to one of ordinary skill in the art at the time the invention was made to ease the candidate function selection condition by changing said reference by a predetermined width and executing the evaluation process and selecting process again, since it has been determined that the invention is designed to find the most suitable s-box design. It would have only required routine skill in the art to repeat the process for every cryptanalysis technique. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

31. Regarding claims 19, 26, 31, and 32, Kim teaches wherein said candidate functions are each a composite function composed of at least one function resistant to said differential cryptanalysis and said linear cryptanalysis and at least one function of an algebraic structure different from that of said at least one function (column 4, lines 12-62).

Art Unit: 2131

32. With regards to claims 23, Kim teaches disclosing evaluating differential-cryptanalysis resistance. **Markov Ciphers and Differential Cryptanalysis**, by Xuejia Lai, discloses that calculating means, for the function $S(x)$ to be evaluated, the number of inputs x that satisfy $S(x) + S(x + \Delta x) = \Delta y$ for every set $(\Delta x, \Delta y)$ and evaluating the resistance of said function to differential cryptanalysis based on the result of said calculation is part of differential cryptanalysis in at least **Section 2. Differential Cryptanalysis of Iterated Ciphers**, on pages 19-22.

33. Kim discloses linear-cryptanalysis resistance evaluating means for calculating, for the function to be evaluated, the number of input values x for which the inner product of the input value x and its mask value Δx is equal to the inner product of a function output value $S(x)$ and its mask value Δy and evaluating the resistance of said function to linear cryptanalysis based on the result of said calculation (Figures 7-9; column 4, lines 19-62).

Conclusion

34. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

35. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

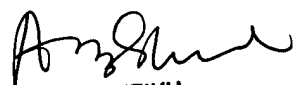
36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

37. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

38. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TEC. CENTER 2100